SIDROPS
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

J. Shi
Tsinghua University
L. Liu
L. Qin
Zhongguancun Laboratory
D. Li
Tsinghua University

2 March 2026

Considerations for On-Demand Retrieval of Multiple RPKI Object Types
draft-shi-sidrops-rpki-on-demand-01

Abstract

Currently, Relying Parties (RPs) retrieve the complete set of RPKI objects from repositories. This all-or-nothing model increases network traffic, synchronization latency, and computational overhead. This document examines these limitations and outlines directions for enabling more selective and efficient RPKI data access.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI) [RFC6480] provides a framework for validating the authenticity and integrity of routing information. It relies on cryptographically verifiable objects published at Publication Points (PPs), which Relying Parties (RPs) retrieve and process to support route validation.

Current RPKI data retrieval assumes that RPs synchronize and cache the complete repository contents. The diversity of RPKI signed objects is expected to grow; beyond ROAs [RFC9582], new object types such as ASPAs [I-D.ietf-sidrops-aspa-verification] and MOAs [I-D.ietf-sidrops-moa-profile] have already been proposed. Existing RP implementations do not support selective retrieval by object type. Consequently, operators that require only a subset of objects must still download and process the entire repository, increasing network traffic, synchronization latency, and computational overhead. For example, an AS that only requires Route Origin Authorizations (ROAs) will also download and process unrelated objects such as ASPAs and MOAs.

This document analyzes these limitations and discusses directions for enabling selective, on-demand retrieval of RPKI objects to improve scalability and operational efficiency.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Problem Statement

As the diversity and volume of RPKI objects grow, there would be an increasing need for RPs to retrieve only the objects of the required type in order to reduce unnecessary overhead. However, current RPKI transport protocols assume full repository synchronization. As a result, networks must download and process signed objects that are not required for their operational needs.

Operational measurements indicate that the current RPKI repository contains roughly 340,000 ROA objects, totaling approximately 655 MB. Assuming the deployment of 70,000 ASPA objects of similar size per object, the additional data would amount to roughly 135 MB. For networks that only require ROAs, retrieving unrelated ASPA objects imposes unnecessary network traffic consumption and computational overhead. As new object types such as MOAs are introduced, these inefficiencies will increase further.

3. Directions and Design Considerations

Type-based on-demand retrieval refers to the ability for RPs to selectively retrieve specific categories of RPKI signed objects. This section discusses high-level directions and design considerations for enabling such on-demand retrieval within existing RPKI transport protocols, including Rsync [RSYNC], RRDP [RFC8182], and Eric Synchronization Protocol [I-D.ietf-sidrops-rpki-erik-protocol].

3.1. Rsync and RRDP

Both Rsync and RRDP currently do not support type-based on-demand retrieval of RPKI signed objects, because neither protocol provides object-level granularity for fetching. An RP must first retrieve all updated objects before it can parse and identify specific object types. As a result, selective on-demand retrieval by object type is not achievable with current designs.

To enable type-based on-demand retrieval, changes may be needed on the PP side, such as reorganizing repository files or exposing explicit object type metadata. With such modifications, RPs could

fetch objects of a specific type without downloading the entire repository. Care must be taken to ensure that these changes do not introduce significant complexity or additional transport overhead.

3.2. Eric Synchronization Protocol

The Erik Synchronization Protocol uses Merkle trees to detect differences between local and remote datasets, enabling RPs to efficiently identify and retrieve only objects that are missing or out of sync.

Although the current specification does not explicitly address on-demand retrieval by RPKI object type, Erik's object-level granularity and manifest-driven design naturally support this functionality. By leveraging object file names in manifests, RPs can filter and fetch only the required categories of signed objects.

4. Security Considerations

This document does not define new protocols, protocol extensions, or modifications to existing RPKI validation procedures or security mechanisms. Therefore, this document does not introduce new security considerations.

5. IANA Considerations

This document has no IANA requirements.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-24, 19 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-24>.

[I-D.ietf-sidrops-moa-profile] Xie, C., Dong, G., Li, X., Huston, G., and D. Ma, "A Profile for Mapping Origin Authorizations (MOAs)", Work in Progress, Internet-Draft, draft-ietf-sidrops-moa-profile-03, 11 January 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-moa-profile-03>.

[I-D.ietf-sidrops-rpki-erik-protocol] Snijders, J., Bruijnzeels, T., Harrison, T., and W. Ohgai, "The Erik Synchronization Protocol for use with the Resource Public Key Infrastructure (RPKI)", Work in Progress, Internet-Draft, draft-ietf-sidrops-rpki-erik-protocol-03, 27 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-rpki-erik-protocol-03>.

[RSYNC] "The rsync web pages", n.d., <https://rsync.samba.org>.

Authors' Addresses

Jiayi Shi
Tsinghua University
Beijing
China
Email: sjy23@mails.tsinghua.edu.cn

Libin Liu
Zhongguancun Laboratory
Beijing
China
Email: liulb@zgclab.edu.cn

Lancheng Qin
Zhongguancun Laboratory
Beijing
China
Email: qinlc@mail.zgclab.edu.cn

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn